AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT	1. CONTRACT ID CODE	PAGE **1** OF **2**

2. AMENDMENT/MODIFICATION NO. **P00002**	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO. **21437144**	5. PROJECT NO. (If applicable)

6. ISSUED BY CODE **47QFCA**

GSA/FEDSIM Acquisition (QF0B1D)
1800 F Street, NW, 3100
Washington, DC 20405
Contract Specialist Name: Millicent Hawkins
Contract Specialist Phone: 703-605-3654

7. ADMINISTERED BY (If other than item 6) CODE

8. NAME AND ADDRESS OF CONTRACTOR (No., Street, County, State and ZIP Code)

GENERAL DYNAMICS INFORMATION TECHNOLOGY, INC.
3150 FAIRVIEW PARK DR STE 100
FALLS CHURCH, VA, 22042-4504
Phone: 703-995-5373 Fax: 703-995-6767

CODE FACILITY CODE

(X)	
	9A. AMENDMENT OF SOLICITATION NO.
	9B. DATED (SEE ITEM 11)
X	10A. MODIFICATION OF CONTRACT/ORDER NO. **47QTCK18D0003 / 47QFCA20F0018**
	10B. DATED (SEE ITEM 13) **08/05/2020**

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

□ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers □ is extended, □ is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing items 8 and 15, and returning ____ copies of the amendment; (b) By acknowledge receipt of this amendment on each of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment your desire to change an offer already submitted, such change may be made by telegram or letter provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and data specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

285F.Q00FB000.AA10.25.AF151.H08 Total Amount of MOD: $0.00

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
X	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF: **In accordance with FAR 43.103(a)**
	D. OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor □ is not, ☒ is required to sign this document and return ____ copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

The purpose of this modification is to: Update Task Order Sections C.3 and F.2. See the attached SF-30 Continuation Page and Conformed Task Order for more details.

Except as provided herein, all terms and conditions of the document referenced in item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print) Keishonna M. Harper, Sr Manager, Contracts		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) **Kristen L Jaremback**	
15B. CONTRACTOR/OFFEROR (b) (6) (Signature of person authorized to sign)	15C. DATE SIGNED 30 Oct 2020	16B. UNITED STATES OF AMERICA (Signature of Contracting Officer)	16C. DATE SIGNED

TASK ORDER (TO)

47QFCA20F0018

Special Operations Forces (SOF) Information Technology Enterprise Contract J (SITEC J) Support

in support of:

The United States Government (USG) Program Office

Issued to:

General Dynamics Information Technology, Inc.

Issued by:
The Federal Systems Integration and Management Center (FEDSIM)
1800 F Street, NW (QF0B)
Washington, D.C. 20405

Awarded August 5, 2020

FEDSIM Project Number DE01066

.C.1 BACKGROUND

The United States Government (USG) Program Office's mission involves providing fully capable Special Operations Forces (SOF) to defend the United States and its interests, and to plan and synchronize operations against terrorist networks. The USG Program Office is responsible for training and equipping all Department of Defense (DoD) SOF to perform missions anywhere in the world at any time. Specific responsibilities of the USG Program Office include developing, acquiring, integrating, fielding, and supporting special operations unique equipment, material, supplies and systems and ensuring the interoperability of equipment and forces.

This TO will provide direct support to the USG Program Office enabling rapid aggregation, fusion, and dissemination of operational information, intelligence, and technology to respond to emerging threats. The USG Program Office solves emerging analytical problems through implementation of custom-developed Information Technology (IT) capabilities as well as by operationalizing advanced technologies from public, private, and academic sectors.

The SITEC J acquisition will contribute to enhance the USG Program Office's ability to support its mission. SITEC J will result in continued development of an enterprise-wide, information-age transformation by building the foundation for increased operations efficiency, capabilities, and delivery flexibility through standardized and consistently-applied policies, procedures, oversight, resource allocation, and the provision of value-added support.

The USG Program Office requires this SOF SITEC J TO for continuing mission critical support for the Operations and Maintenance (O&M) of the Command's IT environment and full breadth of requirements. Through this SITEC J acquisition, the USG Program Office seeks IT services from a service provider covering the full spectrum of IT requirements on a global scale. To contribute to the USG Program Office's mission achievement, IT services must be well-integrated, flexible, and adaptable across all IT service areas, with the ability to rapidly scale in response to the USG Program Office's dynamic mission requirements.

C.1.1 PURPOSE

The purpose of this TO is to provide the USG Program Office with a full range of SOF Enterprise IT services, O&M and support services to SITEC J mission capabilities.

C.2 SCOPE

The scope of this TO includes the full range of SOF IT Enterprise services for unclassified networks Secret/Alternative Compensatory Control Measures (ACCM) networks, Tactical Collateral Secret (TCS), Top Secret (TS)/Sensitive Compartmented Information (SCI) in a dynamic SOF environment across the globe. SOF IT Enterprise Services include Data Center Architect/Engineering support, private and public Cloud Computing support utilizing a hybrid approach with technologies, Application and Database Administration, Enterprise Network Architecture/Engineering, Enterprise Wide Area Network (WAN), Enterprise Voice Architecture/Engineering, Wired and Wireless Network Engineering support, Enterprise Audio/Visual Architect/Engineering, Circuit Actions support, Remote Network Engineering/Installations support to including logistics support, Bulk Encryption Architect/Engineering, Distributed Computing (Desktop) support, IT Service Desk, Cyber Security (CS), Security Operations Center, telecommunications, satellite engineering and support, business analysis, Application Development, Video Teleconferencing (VTC), and Executive Communications (Exec Comms) utilizing Enterprise Mobility Suite. The TO scope also includes providing IT support to deployed forces as required by world events and requirements.

C.3 CURRENT INFORMATION TECHNOLOGY NETWORK ENVIRONMENT

The current SOF Information Environment (SIE) consists of a routed network of user locations, VTC suites, Intelligence Surveillance and Reconnaissance (ISR) platforms, data centers, cloud as service delivery points and related back end hardware and software, processing nodes, Continuity of Operations (COOP) site which includes Disaster Recovery (DR), data ingest points, data exfiltration points in multiple Continental United States (CONUS) and Outside CONUS (OCONUS) locations, Areas of Active Hostilities (AAH), Outside Declared Theater of Active Armed Conflict (ODTAAC), and Forward Operating Bases (FOB). This environment combines multiple virtual and physical server platforms running Operating Standards (OS) that include Microsoft (MS), MacOS, and Linux (as well as derivations thereof), with diversified storage technologies implemented throughout the environment.

This SOF SIE also supports worldwide IT infrastructure. The SIE encompasses all SOF IT assets throughout the USG Program Office, down to the deployed sensor and shooter. The SIE houses the USG Program Office's data centers and related enterprise services, as well as SOF's global terrestrial and satellite connectivity. The interconnected IT systems provide the integration of information, applications, and processes throughout the USG Program Office's global operations as well as across DoD organizational boundaries.

The SITEC J contractor will support the USG Program Office by providing local and remote support to operations around the globe. The USG Program Office provides a globally connected infrastructure distributed across security/classification domains, special purpose networks, development environments, staging and testing environments, and a data-center to support the SITEC J mission IT capabilities. Deployed IT capabilities are an extension of the SITEC J enterprise that provide a remote, self-contained desktop, mission IT analytical tool suite, and communications equipment to deployed analysts. Deployed IT capabilities are designed to operate in austere, remote locations with minimal or no local IT support. These capabilities generally consist of a standardized platform and suite of communications and analytical software tools that are customized to meet the requirements of each operational location. Components may include ruggedized laptops, satellite data and voice equipment, modems, monitors, mobile or satellite phones, Type one or Suite B encryption, peripherals, external hard drives, token readers, switches, hubs, transceivers, backpacks, commercial and Government software suites, shipping containers, spare parts and miscellaneous items. The USG Program Office supports connectivity to sites including Combatant Commands (COCOMs) and Theatre Special Operations Command (TSOCs).

The USG Program Office currently supports approximately 24,000 users who operate on the USG Program Office domains at several service locations including Fort (Ft.) Bragg, North Carolina (NC) (which has two separate, secure compounds, referred to as Site J and Site D); Virginia Beach, VA (Site E); Ft Eustis, Virginia (VA) (Site X); and two locations within the National Capital Region (Sites N and N2); a DR Center controlled from Site J located at Wright-Patterson Air Force Base (AFB), Ohio (OH) (Site W); CONUS field training locations; forward-deployed OCONUS locations including AAH as well as areas ODTAAC. Performance of tasks may be required while on board vehicles, aircraft, or vessels. All USG Program Office users require access to unclassified and classified networks. The USG Program Office IT Enterprise mission infrastructure includes local area networks and enclaves (e.g., Unclassified, Secret, and TS/SCI), connections to DoD enterprise networks, and interconnections to remote USG Program Office CONUS and OCONUS locations.

The USG Program Office manages the acquisition, transition, coordination, and ongoing management of all IT service areas. The USG Program Office will govern the existing capabilities for the enterprise-wide IT Service Management (ITSM) and delivery standards. The USG Program Office translates the SITEC J strategic IT mission objectives into executable operational actions and managing the day-to-day service integration and performance in order to achieve the Command's mission objectives. The service areas that provide enterprise-wide consistency and standardization in support of these major services are as follows:

a. O&M and continuous enhancement of the USG Program Offices IT computing systems, as well as the evolution or replacement of these systems, to achieve the target state SIE through an ongoing series of integrated and interdependent engineering activities;
b. Multi-tier, end-user support of over 24,000 SITEC J users in every country where the USG Program Office has a presence on a 24-hour, 365-days a year basis using multiple communications channels, including telephone (Plain Old Telephone System (POTS) and Voice Over Internet Protocol (VOIP)), email, web chat, voice and VTC; and other support functions and requirements;
c. O&M of all production networks, production security/cyber operations/applications and production workstations used directly in the management and operation of the USG Program Office's global IT environment; and
d. O&M of all development networks and development workstations used directly in the management and operation of the USG Program Office's global development IT environment

Transport technologies connecting the various locations include terrestrial optical, copper, and Radio Frequency (RF) circuits and non-terrestrial RF links including satellite and other platforms. These links have optimization technologies implemented on them to reduce the overall requirement for throughput and prioritize mission critical traffic. Networking technologies include software defined networks, dynamic and static routing technologies, Multi-Protocol Label Switching (MPLS) and diversified switching and routing hardware and software including Juniper, Cisco, F5 and others. Endpoints are both physical and virtual, and include hybrid devices. Desktop virtualization technologies are utilized, increasing security and reducing touch-maintenance. Voice and video endpoints are deployed throughout the enterprise on multiple networks, including POTS, VOIP, VTC, and network connected radios. There is a complete private hybrid cloud environment within the development division allowing for rapid integration and testing of new technologies, both physical and virtual. Within this development environment, there is a full virtual and physical lab at sites J, D and E for software development, CS scanning, testing, and integration of custom developed products. This lab replicates the production environment to the greatest extent possible. Some cloud services are available on the production network with the goal of full integration in the near future. A broad range of CS products and specialists protect the environment from internal and external threats.

C.4 OBJECTIVE

The objective of this TO is to provide integrated IT solutions to support the sustainment of the SOF IT Enterprise as well as solutions to rapidly respond to changing requirements and SOF priorities. The contractor is required to provide a solution that meets the requirements identified below and that will meet rapidly evolving future requirements. This solution shall include modifying, changing, advancing, replacing, supplementing, enhancing, and other supporting capabilities over time with rapid development and implementation.

C.5 TASKS

The following tasks are contained in this TO:

a. Task 1 – Provide Program Management Support

b. Task 2 – Provide IT Enterprise Support

c. Task 3 – Provide Customer Support Services and Solutions

d. Task 4 – Provide Deployed IT Capabilities

e. Task 5 – Provide Global Command and Control System (GCCS) and Air Defense System Integrator (ADSI) Support (Optional Task)

f. Task 6 – Provide Surge Support (Optional Task)

C.5.1 TASK 1 – PROVIDE PROGRAM MANAGEMENT SUPPORT

The contractor shall provide program management support. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified.

C.5.1.1 SUBTASK 1.1 – COORDINATE A PROJECT KICK-OFF MEETING

The contractor shall schedule, coordinate, and host a Project Kick-Off Meeting at a location approved by the Government (Section F, Deliverable 02). The meeting will provide an introduction between contractor and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include all contractor Key Personnel, representatives from the directorates, the USG Program Office Technical Point of Contact (TPOC), other relevant Government personnel, and the FEDSIM COR.

The contractor shall provide a Kick-Off Meeting Agenda (Section F, Deliverable 01) for review and approval by the FEDSIM COR and the USG Program TPOC prior to finalizing. The contractor shall ensure that the agenda includes, at a minimum, the following:

a. Points of contact (POCs) for all parties;

b. Project Management Plan (PMP) (Section F, Deliverable 07) and discussion including schedule and tasks;

c. Personnel discussion (i.e., roles and responsibilities and lines of communication between contractor and Government);

d. Staffing Plan and status;

e. Transition-In Plan (Section F, Deliverable 11) and discussion;
f. Security discussion and requirements (i.e., building access, badges, Common Access Cards (CACs));
g. Invoicing requirements; and
h. Updated Baseline Quality Management Plan (QMP) (Section F, Deliverable 09)

The Government will provide the contractor with the number of Government participants for the Kick-Off Meeting and the contractor shall provide a sufficient number of copies of the presentation for all present.

The contractor shall provide a Kick-Off Meeting Minutes Report (Section F, Deliverable 03) documenting the Kick-Off Meeting discussion and capturing any action items.

C.5.1.2 SUBTASK 1.2 – PREPARE WEEKLY STATUS REVIEWS (WSR) AND MEETING MINUTES

The contractor shall develop and provide a WSR (Section F, Deliverable 15). The WSR shall include the following:

a. Personnel gains, losses, and status (security clearance, etc.), including closeout activities as required by the USG Program Office;
b. Identify personnel that are projected to be absent longer than two weeks (leave, military duty, etc.);
c. Progress updates and demonstrations;
d. TO schedule updates; and
e. List of required Government actions

C.5.1.3 SUBTASK 1.3 – PREPARE A MONTHLY STATUS REPORT (MSR)

The contractor shall develop and provide an MSR (Section J, Attachment E) (Section F, Deliverable 04). The MSR shall include the following:

a. Activities during reporting period, by task (include ongoing activities, new activities, and activities completed, and progress to date on all above mentioned activities). Each section shall start with a brief description of the task;
b. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them;
c. Government actions required;
d. Schedule (show major tasks, milestones, and deliverables; planned, actual, and completion dates for each);
e. Summary of trips taken, conferences attended, etc. (attach Trip Reports (Section J, Attachment F) to the MSR for reporting period);
f. Accumulated invoiced cost for each CLIN up to the previous month; and
g. Projected cost of each CLIN for the current month

C.5.1.4 SUBTASK 1.4 – CONVENE TECHNICAL STATUS MEETINGS

The contractor Program Manager (PM) shall convene a Monthly Technical Status Meeting with the USG Program Office TPOC, FEDSIM COR, and other Government stakeholders (Section F, Deliverable 05). The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and MSR, provide opportunities to identify other activities,to establish priorities, and to coordinate resolution of identified problems or opportunities and ensure that captured requirements meet mission needs. The contractor PM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the FEDSIM COR (Section F, Deliverable 06).

C.5.1.5 SUBTASK 1.5 – PREPARE AND UPDATE A PROJECT MANAGEMENT PLAN (PMP)

The contractor shall document all support requirements in a PMP. The contractor shall provide the Government with the PMP (Section F, Deliverable 07) on which the Government will make comments. The PMP shall incorporate the Government's comments.

The PMP shall include the following:

a. Description of the proposed management approach;
b. Detailed Standard Operating Procedures (SOPs) for all tasks;
c. Milestones, tasks, and subtasks required in this TO;
d. Overall Work Breakdown Structure (WBS) with a minimum of three levels and associated responsibilities and partnerships between Government organizations;
e. Description detailing the contractor's approach to risk management under this TO; and
f. A description detailing the contractor's approach to communications, including processes, procedures, communication approach, and other rules of engagement between the contractor, the Government, and other contractors at the enterprise level

The contractor shall work from the latest Government-approved version of the PMP at all times.

C.5.1.6 SUBTASK 1.6 – PREPARE TRIP REPORTS

The Government will identify the need for a trip report when the request for travel is submitted (Section F, Deliverable 08). The contractor shall keep a summary of all long-distance travel including the name of the employee, location of travel, duration of trip, and POC at travel location. Trip reports shall also contain Government approval authority, total cost of the trip, a detailed description of the purpose of the trip, and knowledge gained. At a minimum, trip reports shall be prepared with the information provided in Section J, Attachment F.

C.5.1.7 SUBTASK 1.7 – PROVIDE QUALITY MANAGEMENT

The contractor shall identify and implement its approach for providing and ensuring quality throughout its solution to meet the requirements of the TO. The contractor shall provide a QMP and maintain and update it as changes in the program processes are identified (Section F, Deliverable 10). The contractor's QMP shall describe the application of the appropriate methodology (i.e., quality control or quality assurance) for accomplishing TO performance expectations and objectives. The QMP shall describe how the appropriate methodology integrates with the Government's requirements. The Government will monitor the contractor's administration of its QMP in accordance with a Quality Assurance Surveillance Plan (QASP).

C.5.1.8 SUBTASK 1.8 – SECURITY EDUCATION

The contractor shall provide a Security Education Plan (Section F, Deliverable 14). The plan shall identify activities that will ensure all contractor personnel assigned to the program fully understand the sponsor's security requirements, any requirements specific to the business areas serviced under this acquisition, and the consequences of non-compliance. The plan shall also include, but shall not be limited to, providing continuing security awareness; debriefing personnel departing the program in a timely manner; ensuring the proper handling of classified data, program-specific data, and Government information; ensuring proper control and classification of program documentation and data; and identifying a process for providing timely notification of security-related issues to the cognizant Government security personnel and an email confirming delivery to the cognizant security personnel to the FEDSIM COR, including a feedback loop for corrective actions taken.

C.5.1.9 SUBTASK 1.9 – ACCOUNTING FOR CONTRACTOR MANPOWER REPORTING

The contractor shall report all contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract via a secure data collection site: the Enterprise Contractor Manpower Reporting Application (ECMRA). The contractor shall completely fill in all required data fields using the following web address:

http://www.ecmra.mil/

Reporting inputs will be for the labor executed during the period of performance during each Government Fiscal Year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported No Later Than (NLT) October 31 of each calendar year. Contractors may direct questions to the support desk at:

http://www.ecmra.mil/

Contractors may use Extensible Markup Language (XML) data transfer to the database server or fill in the fields on the website. The XML direct transfer is a format for transferring files from a contractor's systems to the secure website without the need for separate data entries for each required data element at the website. The specific formats for the XML direct transfer may be downloaded from the web.

The contractor shall provide the Annual Contractor Manpower Report (Section F, Deliverable 16) by completely filling in all the information in the format using the following url:

http://www.ecmra.mil/

C.5.1.10 SUBTASK 1.10 – TRANSITION-IN

After award, the Government will provide comments to the contractor's proposed transition plan. After receipt of the Government's comments, the contractor shall provide its Final Transition-In Plan (Section F, Deliverable 11). The contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition. The contractor shall implement its Transition-In Plan NLT the Project Start (PS) date and all transition activities shall be completed 90 calendar days after TOA.

C.5.1.11 SUBTASK 1.11 – TRANSITION-OUT

The contractor shall provide transition-out support when required by the Government. The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to incoming contractor and to Government personnel at the expiration of the TO. The contractor shall provide a Transition-Out Plan (Section F, Deliverable 12). The contractor shall also review and update the Transition-Out Plan (Section F, Deliverable 13). During Option Period Four, specifically, the Section F, Deliverable 13 Transition-Out Plan shall be reviewed and updated quarterly unless the contractor receives notice by the FEDSIM CO at an earlier date of the need to update (e.g., in the event that an option were not to be exercised).

In the Transition-Out Plan, the contractor shall identify how it will coordinate with the incoming contractor and Government personnel to transfer knowledge regarding the following:

a. Project management processes;
b. POCs;
c. Location of technical and project management documentation;
d. Status of ongoing technical initiatives;
e. Appropriate contractor to contractor coordination to ensure a seamless transition;
f. Transition of Key Personnel;
g. Schedules and milestones; and
h. Actions required of the Government

The contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings or as often as necessary to ensure a seamless transition-out.

The contractor shall implement its Transition-Out Plan NLT 90 days prior to expiration of the TO or as required by the FEDSIM CO.

C.5.2 TASK 2 – PROVIDE IT ENTERPRISE SUPPORT

The contractor shall provide SITEC J support services in order to effectively enable delivery of mission capabilities to internal mission functions in compliance with emerging mission requirements, Government direction, and DoD requirements. The contractor shall ensure the SITEC J Enterprise remains secure, compliant, and available to authorized users 24 hours per day, seven days per week, and 365 days per year (24x7x365). The contractor shall ensure the path to the production environment for mission capabilities is continuously optimized to accelerate delivery of capability to users and warfighters. The contractor shall ensure deployed capabilities are integrated, delivered and supported to meet the mission, functional and schedule requirements of deployed forces.

C.5.2.1 SUBTASK 2.1 – PROVIDE IT ARCHITECTURE AND ENGINEERING SUPPORT

The contractor shall provide IT infrastructure-related architecture and engineering support.

The contractor shall be responsible for the following:

a. Supporting infrastructure-related architecture, engineering, and security architecture;

b. Ensuring that the SITEC J IT infrastructure is optimized to support IT capabilities and is aligned with SITEC J Concept of Operations (CONOPS) to effectively address emerging mission requirements;
c. Designing and engineering the SITEC J IT infrastructure to eliminate single points of failure, optimize quality of service, and to maximize availability of capabilities to SITEC J internal and external users;
d. Supporting IT architecture and engineering for IT Enterprise COOP/DR, and service availability;
e. Supporting and assisting the USG Program Office in implementing the SITEC J enterprise IT technical strategy;
f. Leading special technology projects (e.g., advanced technology evaluations, proofs of concept, and implementation planning) required by the USG Program Office TPOC;
g. Providing technical support to the USG Program Office engagements, technical exchanges, product demonstrations, conferences, capability overviews, and briefings internally within SITEC J and externally to SITEC J partners;
h. Supporting meetings, delivering briefings, and providing demonstrations to Senior Executives and Flag Officers;
i. Providing technical advice and engineering guidance for next-generation planning efforts, including integration with other enterprise services; and
j. Preparing Plans, Designs, Surveys, and Briefings (Section F, Deliverable 17) and technical materials including DoD Architecture Framework Artifacts (Section F, Deliverable 18) as required by the USG Program Office TPOC

C.5.2.1.1 SUBTASK 2.1.1 – PROVIDE IT ENTERPRISE ENGINEERING SUPPORT

The contractor shall improve system and infrastructure efficiency and effectiveness through engineering support services The contractor shall be responsible for the following:

a. Performing system and network engineering, including:
    i. Implementation of technology to support Development Operations (DevOps) enabled capability delivery;
    ii. Engineering and re-engineering infrastructure due to reorganization (e.g., an organization adding a new building, removing a new building or expanding to a new location);
    iii. Replicating or migrating SITEC J IT capabilities, data, and network services to other locations or domains; and
    iv. Planning and implementing transition from internally hosted IT services and mission capabilities to the Defense Information System Agency (DISA) or Intelligence Community (IC) enterprise services or hosting sites as required by the USG Program Office TPOC
b. Designing, engineering, and supporting data replication to local and remote DR systems;
c. Planning and implementing mission capabilities and transition to enterprise services, virtualized and cloud-based technologies. SITEC J is continually assessing options to fully transition IT services to cloud-based solutions in compliance with DoD mandates or

to achieve performance efficiencies and improvements. SITEC J requires the contractor to support internally-hosted advanced technologies and to support the Government decision to transition to enterprise services in a cloud environment, and migration of SITEC J IT services to a new hosting service or technology stack in a multi-cloud environment.;

d. Recommending innovations and improvements in the SITEC J domain that may result in increased efficiency, improved services, and reduced costs to the Government;

e. Providing the following technical reports in accordance with Section F regarding the current and projected health of the SITEC J IT Infrastructure:

   i. Plans and procedures for anticipated events such as power outages, weather events, organizational changes, and data calls from Government leadership (Section F, Deliverable 19);

   ii. Trend analysis, incident reports, problem reports, and outage notifications (Section F, Deliverable 20);

   iii. Recommendations and changes for the IT Enterprise (Section F, Deliverable 21); and

   iv. IT Enterprise Descriptive Documentation (Section F, Deliverable 22) that documents and summarizes the architecture, and connectivity

The USG Program Office requires the contractor to support internally-hosted services and to support transition to enterprise services as required by the Government.

C.5.2.1.2 SUBTASK 2.1.2 – PROVIDE COOP/DR IT SUPPORT

The contractor shall provide IT support to SITEC J COOP/DR efforts and site(s), performing services locally, via remote connection to COOP/DR sites, and local travel to remote sites as requested by the Government. Long-distance travel to and on-site services at remote sites may also be required to support SITEC J COOP/DR emerging requirements. The contractor shall develop and execute Plans and Procedures (Section F, Deliverable 19), as required by the Government, for SITEC J DR capabilities. The contractor shall exercise these plans periodically to ensure that safeguards, backups, end-user services, and procedures can provide continuity of mission support services through issues such as natural disasters, power outages, building loss and allow successful recovery of all services after facility restoration or the establishment of an alternate facility.

The contractor shall provide the following DR-related services as required by the Government:

a. Provide technical support to SITEC J DR meetings;

b. Support technical assessment and perform site surveys for DR candidate sites and hosting services in support of Government planning activities;

c. Produce written Plans, Designs, Surveys, and Briefings (Section F, Deliverable 17) to assist the USG Program Office in developing and documenting DR capabilities;

d. Provide IT technical liaison and coordination and Tier III support with COOP/DR (one and the same) facility service providers. Given the interdependence of IT components, collaboration is required and is an important objective;

e. Support and administer network connectivity, encryption, circuits, and other communications systems between the USG Program Office and DR facilities;
f. Provide IT-related technical support to the operation of the USG Program Office DR capabilities; and
g. Support implementation, configuration, and administration of DR systems (virtual or physical) that fall within the USG Program Office's IT management control, authorization boundaries, and operate as an extension of the SITEC J enterprise

The contractor shall provide the following COOP-related services as required by the Government:

a. Provide IT-related technical input to the USG Program Office COOP planning, design, and implementation efforts, including meeting and briefing support;
b. Support and administer network connectivity, encryption, circuits, and other communications systems between the USG Program Office and COOP facilities; and
c. Support implementation, configuration, and O&M of SITEC J systems, services, and mission capabilities for COOP IT assets that fall within the USG Program Office's management control, security boundaries, and operate as an extension of the SITEC J enterprise

C.5.2.1.3 SUBTASK 2.1.3 – PROVIDE PROOF OF CONCEPT, PROTOTYPING, AND PERFORMANCE OPTIMIZATION

The contractor shall support the USG Program Office mission in innovative technologies and mission capabilities by leveraging and implementing advanced capabilities, methodologies, technologies, and subject matter expertise from public, commercial, and academic sectors that may be conceptual, experimental, or the product of the USG Program Office programs. The contractor shall advise Government personnel of relevant new or emerging technologies, perform technology assessments, and provide performance-enhancing recommendations as requested by the Government. Examples include delivery of new IT capabilities and future alignment of SITEC J IT Enterprise infrastructure with DoD or IC enterprises.

The contractor shall continuously assess and optimize performance of the IT Enterprise, including the path and process by which mission capabilities are introduced into the USG Program Office production environments. In collaboration with other USG Program Office organizations (e.g., IT Enterprise, Configuration Management, etc.) the contractor shall optimize and automate the IT capability path to production to accelerate response to mission requirements and delivery of new capabilities. For example, the contractor shall implement and provide O&M of DevOps enabled technologies and capability delivery methodologies.

The deliverables required for this work may take many forms such as information papers, service catalogues, process and procedure documentation, briefings, and training packages. (Section F, Deliverable 19).

C.5.2.1.4 SUBTASK 2.1.4 – PROVIDE SYSTEM ENGINEERING TECHNICAL SUPPORT

The contractor shall perform the following:

a. Provide systems engineering technical support for Exec Comms in a mature environment from planning & design through deployment to ensure that the USG Program Office enables their internal and external users to meet mission goals and objectives. These efforts include the full range of infrastructure engineering design, enterprise architecture standards, prototyping, integration, concept development, planning, requirements definition and analysis, systems design, integration, and deployment. Examples include Apple, Android, Choose Your Own Device (CYOD), VOIP and proprietary devices that could be used to provide services to the executive staff. Existing systems infrastructure consists of Blackberry Exchange Services (BES12), MS Outlook, MS Lync, Cisco Jabber, Cisco AnyConnect, and associated hardware and software. Existing infrastructure consists of a variety of Mobility Suites, including MS, VMware, Cisco, HYPORI and others.; and

b. Provide on-site Tier II technical support for Android Tactical Assault Kit (ATAK) and other Android based mobile devices. These efforts include maintaining baselines, configuration, maintenance, and documentation for mobile devices. Examples include ATAK, Android based handsets and tablets and proprietary mobile devices that could be used to provide services.

C.5.2.2 SUBTASK 2.2 – PROVIDE IT ENTERPRISE O&M

The contractor shall perform the Enterprise O&M work described below for all SITEC J IT infrastructure and systems as required by the Government.

C.5.2.2.1 SUBTASK 2.2.1 – PROVIDE NETWORK AND SYSTEMS OPERATIONS

a. Provide installation, configuration, administration, O&M, and operational availability support to SITEC J infrastructure, applications, user desktops, and mission IT capabilities (e.g., hardware, software, platforms, connectivity) in testing, staging, and production environments;
b. Store, back-up, restore, and archive data on all servers and perform recovery operations as needed;
c. Install, configure, and administer cross-domain solutions, ensuring required separation of roles and administrative duties;
d. Maintain and optimize standard configurations, images, and system baselines on all enclave components;
e. Maintain and administer SITEC J enterprise management tools, such as Solarwinds, MS System, Center Configuration Manager (SCCM), System Center Operations Manager, Splunk;
f. Maintain and operate network and system management software, and other systems such as patch servers, update servers, and storage solutions;
g. Manage storage systems on all infrastructure components;
h. Provide Tier I, II and Tier III network engineering support to maintain network devices to ensure the networks are operating.
i. Provide installation, configuration and maintenance of firewall, intrusion devices and security appliances to ensure that the networks are protected at all times;
j. Provide installation, configuration and maintenance of VOIP devices and systems;

k. Provide installation, configuration and maintenance of encryption devices across networks;
l. Advise the Government on emerging technologies and techniques and procedures;
m. Assist the USG Program Office Development Project branches (two branches) with compiling data and documentation for IA testing;
n. Maintain systems hosted for third-party Government organizations IAW site licensing agreements, interagency agreements, or as requested by the Government (some systems may process data that has restricted access for special access programs requiring read-on by IT personnel);
o. Provide infrastructure O&M for data feeds and data ingest into mission IT production systems;
p. Create and maintain current, written administrative, and system maintenance procedures (Section F, Deliverable 23);
q. Perform acceptance testing to determine suitability of systems and software for operation in the production environment and produce acceptance test reports as requested by the Government (Section F, Deliverable 24);
r. Implement CS corrective actions, patches, bug fixes, and other remediation activities per Plan of Action and Milestone (POA&M) and other requirements to maintain CS compliance;
s. Develop, update, and maintain technical documentation, user guides and “how to” materials to assist SITEC J enterprise users (Section F, Deliverable 25);
t. Draft IT-related guidance and instructions for incorporation into the USG Program Office Fragmentary Order (FRAGO) issuances. FRAGOs serve as internal directives that task Staffs and organizations with action, coordination, and response;
u. Install, implement, and integrate systems hosted for third-party organizations as requested by the Government; and
v. Administer, maintain, customize, and optimize the USG Program Office implementations of ITSM workflow automation solutions (primarily Service Now and SCCM)

C.5.2.2.1.1 SUBTASK 2.2.1.1 – PROVIDE USG PROGRAM OFFICE MAINTENANCE NETWORK SUPPORT

The contractor shall maintain networks to simulate the “Operational Networks” (testbed) at the USG Program Office compound. The branch is process based and the contractor shall ensure that process documentation is current, correct and that the configuration management of the documents is maintained utilizing ServiceNow and SharePoint.

C.5.2.2.1.2 SUBTASK 2.2.1.2 – PROVIDE CONFIGURATION MANAGEMENT (CM) SUPPORT

The contractor shall perform the following CM work:

a. Provide subject matter expertise for all tactical and automation systems in order to manage hardware and software changes to the baseline of all information systems;
b. Ensure information systems compliance with DoD standards and documented reference models;

c. Ensure that all information systems changes are documented against current systems baselines and satisfy validated requirements;
d. Manage the process that identifies, tracks changes, and records/reports the implementation status and any issues resulting from a systems configuration change item; and
e. Maintain the database of all information systems baseline components and provide configuration management summaries to the JCU Chief of Maintenance (Section F, Deliverable 38)

C.5.2.2.1.3 SUBTASK 2.2.1.3 – PROVIDE NETWORK ENGINEERING SUPPORT

The contractor shall perform the following:

a. Provide on-site Tier II and Tier III support for non-SCAMPI Enterprise network infrastructure, while working in conjunction with the Enterprise Network service providers to ensure delivery of Enterprise-wide services. This support shall include all related planning, system architecture, installation, configuration, O&M, documentation, engineering, and CS activities related to network services. These include strategic and tactical planning to identify, manage, direct and translate objectives, requirements, resource constraints, CS risks, and schedule into logical, actionable elements to be implemented to achieve the parameters specified in the strategic plan, provide telecommunications engineering and support, manage virtualized services, and support call manager systems. Tier II Network Engineering support shall be performed 24x7x365 in the Cyber Network Operation Center (CNOC) with at least two staff at all times. The contractor shall provide Tier III "Backshop" support, with after hours, on-call support for escalated issues from the CNOC for over 90 networks; and
b. Provide on-site Tier II and Tier III support for the wireless network. This support shall include all related planning, installation, configuration, O&M, documentation, engineering, and CS activities related to wireless access points, sensors, switches, routers, and gateways. The contractor shall provide technical support for all phases of a secure, wireless system, from planning and design through deployment and O&M to ensure that the USG Program Office enables its internal and external users to meet mission goals and objectives. These efforts include the full range of infrastructure engineering design, enterprise architecture standards, prototyping, and integration, including, concept development, planning, requirements definition and analysis, systems design, integration, and deployment. This includes the integration of the secure wireless network into the existing architecture. Commercial Internet service, unclassified, and secret networks have active wireless access.

C.5.2.2.1.4 SUBTASK 2.2.1.4 – PROVIDE NETWORK ENGINEERING TECHNICAL SUPPORT

The contractor shall provide network engineering technical support for Exec Comms, from planning and design through deployment to facilitate the USG Program Office ability to ensure its internal and external users can meet mission goals and objectives. These contractor efforts include the full range of infrastructure engineering design, enterprise architecture standards, prototyping, integration, concept development, planning, requirements definition and analysis, systems design, integration, and deployment.

C.5.2.2.2 SUBTASK 2.2.2 – PROVIDE INCIDENT, PROBLEM, OUTAGE, AND TROUBLE MANAGEMENT

The contractor shall provide the following incident, problem, outage, and trouble management support:

a. Monitor the mission support infrastructure and capabilities for emerging and actual incidents, problems, outages and other events impacting IT performance and CS status;
b. Provide preventative mitigations to faults and service degradations where possible through proactive measures to address service degradation or interruption for SITEC J users;
c. Provide off-hours remote or call-in support with a one-hour response time for outages to mission capabilities, mission-critical services, infrastructure availability, and SITEC J leadership support (unless otherwise required by the USG Program Office TPOC, IT capabilities at COOP/DR facilities shall be considered mission-critical services with a four-hour response time to outages of COOP/DR systems when the primary facility remains functional);
d. Provide support to the Government's development of After Action Report (AAR) generation activities for outages and incidents that degrade or interrupt mission capability services or core services to users (AARs describe the incident and identify actions taken, potential future preventative actions, and lessons learned). However, in addition to supporting the Government's AAR generation activities, the contractor may be required to generate and deliver ad hoc AAR (Section F, Deliverable 26); and
e. Support the Government's development of an automated dashboard showing the status of the network and system performance, security compliance, and other metrics as requested by the Government

C.5.2.2.3 SUBTASK 2.2.3 – PROVIDE DATA CENTER OPERATIONS AND MANAGEMENT SUPPORT

The contractor shall provide the following data center operations and management support:

a. Support the design, management, operation, and maintenance of the data center in collaboration with IT engineers and administrators, security personnel, and facilities personnel;
b. Develop, update, and maintain technical and operational documentation and diagrams (Section F, Deliverable 27); and
c. Support data center expansion, migration, and other changes in response to changing SITEC J mission requirements

C.5.2.3 SUBTASK 2.3 – PROVIDE CYBERSECURITY SUPPORT SERVICES

The contractor shall provide CS services IAW DoD 8500 series instructions and other applicable DoD and IC publications, and instructions. The contractor shall also provide security engineering support and guidance to ensure that the SITEC J IT Enterprise is compliant with all DoD, IC, DISA and USG Program Office network security controls, patches and imaging: Security Technical Information Guides (STIGs) (currently utilizing Docker), and hot fixes. The contractor shall maintain, track, and report contractor personnel certifications under DoD Instruction (DoDI) 8570.01 and subsequent revisions. The contractor shall comply with the direction of the USG Program Office/SITEC J CS officials, including the Authorizing Official (AO), Security Controls Assessor (SCA), and Information Systems Security Manager (ISSM).

Contractor IT activities shall comply with DoD and IC CS implementation guides, instructions, frameworks, and directives. The contractor shall ensure that CS requirements are treated like other system requirements and are addressed early and continually throughout the IT lifecycle in response to evolving threat, risk, compliance requirements, and mission.

C.5.2.3.1 SUBTASK 2.3.1 – PROVIDE CYBERSECURITY OPERATIONS

The contractor shall ensure that SITEC J IT enclaves and networks operate in compliance with DoD and IC CS Risk Management Frameworks (RMFs), instructions, and directives (e.g., DoDI 8500.01, DoDI 8510.01, IC Directive (ICD) 503), CS warning, and DISA Computer Network Defense (CND) requirements). CND operations shall be staffed on site between the hours of 0800 and 1500 on Government working days. Additional support hours may be required to support incident response, audits, compliance activities, and specials events required by the USG Program Office TPOC to achieve 24x7 defense of SITEC J IT assets. The CNOC is manned 16x5 with staff on-call as necessary.

The contractor shall perform CS services as required, including:

a. Perform local, onsite CND activities for SITEC J enterprise and infrastructure in coordination with the CS Service Provider (CSSP) and parent organization CS functions;
b. Perform general CND activities for SITEC J enterprise and infrastructure;
c. Provide CS technical support to patching, remediation, and POA&M activities for SITEC J IT infrastructure and production systems throughout the SITEC J enterprise;
d. Serve in the role of Information Systems Security Officer (ISSO)
e. Perform security administration, audit log aggregation, and audit analysis;
f. Administer and maintain anti-virus, anti-malware, and host and network-based security software, filters, rules, devices, and device-level policies in collaboration with network engineers and system administrators;
g. Assist the Government in performing incident response, computer emergency response, and support legal investigations and forensic activities;
h. Maintain CS related procedures, administrative guides, and technical documentation (Section F, Deliverable 28);
i. Provide mission IT related security engineering and design guidance support throughout the Software Development Life Cycle;
j. Support SITEC J implementation of the DevOps path to production and support implementation of automated testing and validation capabilities in collaboration with software developers as required by the USG Program Office TPOC;
k. Provide technical briefings and support to security operations-related meetings with the USG Program Office leadership;
l. As requested by the Government, conduct threat assessments and produce threat reports

as required by the USG Program Office, DoD, and IC instructions and frameworks (Section F, Deliverable 39);

m. Support the management of SITEC J Public Key Infrastructure (PKI) hardware, user tokens, and certificates (e.g., SIPRNet CACs, soft or digital certificates for SITEC J servers);
n. The contractor shall maintain a DISA-compliant registration authority and issue SIPRNet CACs on site between the hours of 0800 and 1700 on Government working days (applicable to Site E and Site D – the Government will issue at Site J);
o. Provide security administration and engineering support for guards and cross-domain solutions;
p. Provide reliable human review for transferring data between systems IAW the USG Program Office and DoD policies and procedures;.
q. Provide periodic manual and automated data transfer services including cross-domain file transfers, scans, and reviews for the SITEC J enterprise in response to user and Government requests;
r. Prevent, detect, and mitigate intrusions;
s. Provide liaison and coordinate incident responses with the DoD and IC CS authorities, the USG Program Offices CSSP, and other similar organizations;
t. Support the USG Program Office physical server security efforts, including coordination with physical server security personnel where appropriate;
u. Maintain a current list of authorized privileged users, manage authorization and revocation of privileged users, and ensure least-privilege of user accounts and user awareness of security responsibilities (Section F, Deliverable 29);
v. Support the review of SITEC J user agreements to maintain compliance with evolving DoD and IC requirements;
w. Lead and support efforts for preparation, engagement, and successful outcome of DoD and IC CS inspections and tests; and
x. Support the creation and maintenance of a portal or other automated dashboard to display network and system compliance status and statistics (support the display of compliance status using DoD readiness inspection metrics and other metrics approved by the USG Program Office TPOC)

C.5.2.3.2 SUBTASK 2.3.2 – PROVIDE CYBERSECURITY (CS) RISK MANAGEMENT SUPPORT

The contractor shall support SITEC J risk management activities including authorizations, risk assessments, and threat assessments IAW DoD and IC RMF and processes. The contractor shall draft and staff authorization packages, authorization letters, and other risk management documentation for all SITEC J IT assets (e.g., infrastructure, networks, interconnections, commercial software, custom developed applications, systems, and frameworks).

The contractor shall perform security services throughout the IT lifecycle, including the following:

a. Ensure that risk management packages are developed and maintained concurrently throughout the system life cycle, beginning at inception of new IT activities;

b. Comply and coordinate with the USG Program Office CM processes;
c. Support the USG Program Office CS and risk management officials including the AO, ISSM(s), and SCA as needed; and
d. Execute risk management support and develop packages using processes and templates that are approved by the cognizant risk management official

The contractor shall perform the following Risk Management support services as required by the Government:

a. Support the USG Program Office's efforts to implement and comply with DoD and IC RMF and legacy Certification and Accreditation (C&A) processes, including transition of systems and networks to the RMF;
b. Prepare RMF packages, including security plans, system descriptions, diagrams, data flows, POA&M, security assessment reports, and other documentation (Section F, Deliverable 40);
c. Update and maintain C&A packages that may be required for legacy systems prior to transition to the RMF;
d. Provide technical support to risk assessments and risk determinations, including preparation of technical documentation such as Cybersecurity Impact Assessments (Section F, Deliverable 28) that summarize test results, risks, and threats in support of ISSM, SCA, and AO risk decisions;
e. Provide security engineering support throughout RMF IT lifecycles in coordination with system engineers and software developers. Examples include identification of common controls, system categorization, security control selection, security control tailoring, and providing design and implementation guidance to software developers, system engineers, and network engineers;
f. Review IT system plans, designs, configurations, and architectures for compliance with DoD CS requirements;
g. Assist Government CS officials with design and implementation of RMF workflow, processes, and procedures;
h. Track CS related appointments and maintain current appointment letters (e.g., AO, ISSM, ISSO, SCA, etc.) for signature by the USG Program Office CS officials;
i. Provide coordination, liaison, and support of CS related relationships with external partner organizations, including preparation of CS-related documentation and agreements for interconnections, reciprocity, and the USG Program Office COOP/DR facilities;
j. Assist the Government with its development and maintenance of CS policies and procedures;
k. Support the Government's risk management and approval of commercial, third-party, and open-source software;
l. Support the organization's liaison with DoD and IC CS organizations and reporting to enterprise tracking and compliance systems;
m. Provide technical briefings, meeting support, and status updates related to CS and risk management (Section F, Deliverable 28); and

n. Create, update, and maintain a portal or other form of management dashboard (Section F, Deliverable 27) to automate the tracking and reporting of work queue, status, and performance statistics for documentation packages and other risk-management activities

C.5.2.4 SUBTASK 2.4 – PROVIDE ASSESSMENT AND TESTING SERVICES

The contractor shall ensure that SITEC J mission capabilities, infrastructure, networks, systems, and applications are tested in compliance with the USG Program Office, DoD, and IC instructions, directives, frameworks, and standards. The contractor shall support design and implementation of advanced or automated testing capabilities to accelerate delivery of mission capabilities. The contractor shall provide the USG Program Office Government leads with accurate, objective, and impartial verification of the compliance status of the SITEC J IT enterprise. The contractor shall ensure that SITEC J testing activities are coordinated, planned, and executed as part of IT system lifecycles and projects. The contractor shall provide effective capacity planning and reporting to enable the USG Program Office TPOC to prioritize tasks and focus testing resources on critical SITEC J priorities. The contractor shall contribute to the reporting of information such as test capacity, queues, priorities, completion status, performance statistics, and schedules by creating or leveraging a portal or other automated reporting capability approved by the USG Program Office TPOC.

C.5.2.4.1 SUBTASK 2.4.1 – PROVIDE SECURITY ASSESSMENT AND TEST PLAN SUPPORT

The contractor shall support the preparation and maintenance of assessment and test plans as required by the Government. The assessment and test plans shall describe the methodology by which the contractor shall execute each type of testing and shall contain information as requested and approved by the SCA and the USG Program Office TPOC. The contractor shall propose efficient methods of maintaining test plans to minimize paperwork and cost.

C.5.2.4.2 SUBTASK 2.4.2 – PROVIDE TEST PROCEDURE DEVELOPMENT SUPPORT

The contractor shall identify, develop, and deliver test procedures and test cases (Section F, Deliverable 31) for each new SITEC J software application, widget, system, integration effort, or technology insertion into the IT Enterprise as requested by the Government. Test procedures shall be in compliance with DoD and IC directives, frameworks, and guides (e.g., DoDI 8500 series, DISA Security Technical Implementation Guides, Security Requirements Guides (SRGs)) The contractor shall leverage test procedures, security control assessment procedures, and test tools provided or mandated by the DoD, IC, or other Government entity. This includes continuous monitoring methods in compliance with DoD and the USG Program Office direction. When pre-defined test procedures are not available, the contractor shall propose test procedures for SCA approval and for inclusion in the security assessment report. The contractor shall continuously manage and optimize test methodologies and approaches to improve efficiency and reduce costs.

C.5.2.4.3 SUBTASK 2.4.3 – PROVIDE ASSESSMENT AND TESTING ACTIVITIES

As required by the USG Program Office TPOC, the contractor shall execute approved test procedures to validate the implementation of CS controls and requirements for SITEC J assets.

The contractor shall conduct testing to support authorizations, re-authorizations, periodic network tests/scans, periodic compliance testing, continuous monitoring, and preparation for readiness inspections and audits as requested. The contractor shall re-test or validate bug fixes and other remediation activities identified in previously completed test activities.

The contractor shall conduct security control assessments (both common/inherited controls and system-specific controls) in compliance with DoD and IC CS instructions and RMFs. The contractor shall apply, where feasible, test procedures, methodologies, and tools identified by the DoD and the IC (e.g., DoDI 8500 series, DISA STIGs, DISA SRGs, and DoD's Knowledge Service) The contractor shall support SITEC J continuous monitoring and periodic security control assessments. The contractor shall perform testing of cross-domain solutions using approved test plans in coordination with CS operations personnel.

The contractor shall review and assess software code, review software code scans and assessment reports, and operate software code scanning tools as prescribed by DoD RMFs and technical guides. The contractor shall identify the existence and causes (where feasible) of deficiencies, vulnerabilities, and other findings within software code.

The contractor shall maintain the current USG Program Office testbed environment on each level of network as required by the USG Program Office TPOC and in coordination with the SCA or other Government testing authority. The test environment will be populated with Government-Furnished Equipment (GFE). The contractor shall prepare and update, as required by the Government, a Test Environment Design and Management Plan (Section F, Deliverable 32) for approval by the USG Program Office TPOC. This plan shall contain information such as the design or architecture of the test environments, required tools, hardware, software, administrative procedures, and the contractor's approach to maintaining test environments.

C.5.2.4.4 SUBTASK 2.4.4 – PREPARE ASSESSMENT AND TEST REPORTS

The contractor shall prepare reports that capture all tests, assessments, and results with content and structure as approved by the SCA or the USG Program Office TPOC. Where feasible, the reports shall include technical recommendations for remediation or mitigation of deficiencies. Reports shall include descriptions of deficiencies and their severity to enable risk determinations by the SCA or other personnel. The contractor shall deliver test reports to Government and industry personnel as required by the USG Program Office TPOC (Section F, Deliverable 24). The contractor shall provide technical input to the development of POA&Ms, risk assessment activities, remediation planning, and bug-fix planning. The contractor shall, where feasible, leverage automated test reports or the output of automated tools to improve efficiency and minimize paperwork.

As required by the USG Program Office TPOC, test reports and artifacts shall be prepared as an addendum to or component of risk management packages, security assessment reports, authorization letters, memoranda, or other documentation packages. Artifacts may include output from automated test tools, code scan reports, screen shots that depict aspects of system configuration and other information requested by Government risk management officials.

C.5.3 TASK 3 – PROVIDE CUSTOMER SUPPORT SERVICES AND SOLUTIONS

The contractor shall provide SITEC J users and warfighters highly responsive support services and high-quality IT solutions that result in sustained high customer satisfaction.

The contractor shall provide a wide range of customer services to aid and assist end users and shall employ the capabilities of SITEC J Enterprise to maximize the benefit of the USG Program mission. The contractor shall maintain and report appropriate Task 3 personnel certifications and qualifications under DoDI 8570.01. The contractor shall base customer services and service desk operations on ITSM best practices. The contractor may propose implementation of additional standards, management models, and best practices for approval by the USG Program Office TPOC.

C.5.3.1 SUBTASK 3.1 – PROVIDE SERVICE DESK SERVICES

The contractor shall provide IT service desk support in USG Program Office facilities. Service desk locations are at sites D, E, N, and X and shall also operate during business hours with support on call or surged as required. Although Site J is the primary location, each site must operate as its own independent enterprise and must have its own primary service desk.

Increases or reductions in service desk hours of operation, services, or level of effort may be implemented after coordination among the contractor, FEDSIM COR, and the USG Program Office TPOC. For example, adjustments may be required in support of emerging SITEC J mission requirements, organizational changes or requests for support. Response to these requirements may result in permanent or limited-duration changes to service desk support.

The service desk shall serve as the single, initial contact point for SITEC J users across the enterprise to resolve incidents and problems, including mission IT capabilities, computer security, hardware, software, networks, telecommunications, portal and website platforms, audio-visual, system access, and connectivity for all USG Program Office networks, including SITEC J tenants, deployed sites, and analysis teams. The contractor shall provide dedicated service-desk and IT-technical support to SITEC J (Government and contractors) on site. Work activity may include some or all of the following activities.

a. Open an incident ticket upon receipt of all initial calls and either answer the question, resolve the problem, or forward the problem to the appropriate technical support staff;
b. Verify accuracy of trouble tickets and validate the nature of problem reported. Only close trouble tickets after the issue or problem has been resolved (service desk tickets related to portal and website software not operated by the contractor shall be relayed to the appropriate technical support personnel);
c. Monitor, manage, and optimize user call queues and responses to service desk phone calls;
d. Resolve service requests to the maximum extent possible using remote support tools. Provide touch labor when required;
e. To the extent feasible resolve customer problems and respond to customer requests while on the telephone with the customer;
f. Escalate resolution of the problem according to the USG Program Office TPOC-approved escalation procedures. Provide the caller with a realistic estimate of the time required to resolve the problem;
g. Routinely update and manage assigned trouble tickets. Provide daily ticket queues and Very Important Person (VIP) support status to Government customer service leads via dashboard, email updates, and in person where required;

h. Establish and maintain accounts and passwords for all infrastructure users and control access;
i. Confirm with each customer that his or her problem has been resolved and verify customer satisfaction with the service provided;
j. Develop procedures, provide technical support, and support service-desk solutions for use of DoD and IC enterprise services, allowing for effective delivery and coordination of local SITEC J service desk activities. Interface with the services of the enterprise service provider; and
k. Assess the existing self-help capability and improve or re-develop and maintain an automated, online, easily accessible, user self-help feature, including a Frequently Asked Questions (FAQ) list, with the intent of reducing the need for users to contact the service desk (Section F, Deliverable 35)

C.5.3.1.1 SUBTASK 3.1.1 – PROVIDE TIERS I AND II SYSTEM ADMINISTRATION SUPPORT

The contractor shall provide Tiers I and II systems administration support for operation and maintenance of hardware and software across multiple classifications of networks, maintain system security; execute customer practices and procedures; and monitor usage statistics and logs The contractor shall initiate actions and incident response procedures for systems related problems, address in priority order, troubleshoot, escalate, and track to resolution. Additionally, the contractor shall create accounts; perform hardware setup, port configuration, permissions management, and user trouble shooting; and manage service desk functions.

C.5.3.1.2 SUBTASK 3.1.2 – PROVIDE TIER I, II AND III SERVICE DESK SUPPORT

The contractor shall provide on-site Tiers I, II and III service desk support. The service desk shall receive applicable service requests via the Government designated incident reporting system or by telephone, walk-in, or email. The service desk shall open an incident on behalf of the customer, for metrics. The service desk shall strive for first-call resolution; if beyond the capabilities of the service desk, the service desk shall elevate and assign the work request to the appropriate Tier II or Tier III work center, (i.e., distributed computing (desktop support), System Engineering, Network Engineering, or Applications Management) for resolution. Additional performance is required, historically at two OCONUS sites (currently in the Central Command (CENTCOM) Area of Responsibility (AOR)).

C.5.3.1.3 SUBTASK 3.1.3 – PROVIDE DEPLOYED TIER I AND II SERVICE DESK SUPPORT

The contractor shall provide the following deployed Tier I and II service desk support:

a. Provide deployed Tiers I and II service desk/desktop technicians for *on-site*, 24-hour Tier I and Tier II service desk/desktop support. The service desk shall be available to receive applicable work requests 24x7x365 via the Government-designated ticket system and telephone (if received telephonically, the service desk shall open a work request for the customer). The service desk shall strive for first-call resolution, if beyond the capabilities of the service desk, elevate and assign the work request to the appropriate Tier II work center (i.e., System Engineering, Network Engineering, or Applications Management for resolution). Contractor technicians shall also resolve desktop configuration item incidents and Installation, Moves, Add, Changes (IMACs). Performance is required 24x7x365 including what has been historically required at multiple OCONUS sites (currently in two separate GCC sites).

C.5.3.2 SUBTASK 3.2 – PROVIDE COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS, INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (C4ISR) SUPPORT

The contractor shall perform the following C4ISR support functions:

a. Provide Tier II and Tier III system engineering support for testing new computer hardware, software applications and specialized communication devices on servers and network devices (i.e. physical and virtual) to determine potential use and fielding to the SOF;
b. Provide support to Development Support Branch systems engineers for physical server installation, configuration and maintenance of physical servers, ensuring uninterrupted operations;
c. Provide support for backup and recovery services across the networks with current backup solution systems;
d. Provide support for installation, configuration and maintenance of MS Exchange servers and services and configuration and maintenance of Active Directory Domain Services;
e. Deploy and evaluate custom and Commercial Off-the Shelf (COTS)/Government Off-the Shelf (GOTS) software onto networks to validate deployment instructions and assist with any instruction corrections; and
f. Perform Windows update services, ensuring that server configurations are within Government prescribed standards to include patching, STIGs, and service mapping of the computer systems

C.5.3.3 SUBTASK 3.3 – PROVIDE EMAIL SERVICES

The contractor shall provide email services for multiple security levels in support of the SITEC J mission. Specifically, the contractor shall perform the following:

a. Provide Tier I and Tier II support to DoD’s Non-classified Internet Protocol Router Network (NIPRNet) enterprise email services and future migrations to other enterprise services as required (enterprise email solutions may require support of hybrid solutions comprised of both locally maintained systems and enterprise services);
b. For Secret Internet Protocol Router Network (SIPRNet) and Joint Worldwide Intelligence Communications Systems (JWICs) enterprise email efforts, provide IT planning support, engineering, designs, technical management, coordination, and O&M for migration to and operation of DoD and IC enterprise email services when required by the USG Program Office TPOC;
c. Create and manage email accounts, manage mailbox sizes, and maintain a global active directory that is coordinated with DoD or IC directories;
d. Provide consistent support and functionality for all SITEC J email users regardless of end-user or server operating systems;

e. Provide remote email access as authorized by the Government and coordinate with DoD mobility capabilities and programs;
f. Provide virus checking and spam filtering;
g. Coordinate with DoD and IC enterprise cross-domain email services;
h. Establish, implement, and manage policies concerning naming conventions, distribution lists, send and receive throughput, retention, backup, and data management, IAW the USG Program Office and DoD requirements; and
i. Develop, update, and maintain technical and operational documentation and training materials (Section F, Deliverable 27)

C.5.3.4 SUBTASK 3.4 – PROVIDE AUDIO-VISUAL (AV)/VIDEO TELECONFERENCE (VTC) SUPPORT SERVICES

The contractor shall provide on-site VTC support services at the USG Program Office facilities. The contractor shall coordinate and provide technical support for all SITEC J AV and VTC systems and facilities**.** The USG Program Office leadership meetings, inter-agency VTCs, agency-wide all-hands meetings, and other mission-critical meetings generally require both remote and direct, in-person support throughout the duration of the meeting.

The contractor shall ensure that facilities are operated and maintained IAW organizational security policies and procedures. The contractor shall provide VTC and conference room AV training to Government personnel, such as executive assistants and frequent VTC users. The contractor shall determine AV equipment and VTC facility setup requirements based on user' needs, system capabilities, and accepted production and presentation techniques.

The contractor shall track and manage all AV equipment, software licenses, and maintenance agreements and incorporate AV equipment life cycle planning into the IT O&M deliverable (Section F, Deliverable 41) to ensure that equipment is replaced in a timely and cost-effective manner as requirements emerge or technology improves. The contractor shall also evaluate new technologies and compare to validated requirements, and recommend new equipment, configurations, system enhancements, or technological changes that would result in improved system cost effectiveness and user productivity. The contractor shall install hardware and software related to conference room AV and VTC facilities and maintaining associated network, computers, peripherals, and audio or video equipment. The contractor shall support planning, installation, configuration, and operation of enterprise technologies (e.g., Defense Connect Online, MS Skype, and Tandberg) to improve mission support and to ensure that the USG Program Office achieves maximum value from DoD enterprise solutions. The contractor shall replace equipment as required by the Government. The contractor shall support the following capabilities:

a. Digital video recording;
b. VTC;
c. Knowledge walls, and digital white boards;
d. Webcasts;
e. Defense Chat Online (DCO), MS Lync, and other collaborative technologies; and
f. Commercial and Government collaboration tools

In addition to providing the above capabilities, the contractor shall perform the following:

a. Maintain system reports on utilization, system performance, and maintenance;
b. Prepare facilities for each individual conference and monitor equipment performance during videoconferences. Identify requirements and maintain a plan to provide direct support to the USG Program Office command group. Videoconferences are in the USG Program Office facilities and events occur throughout the day. The contractor shall maintain operating procedures for user support;
c. Determine user visual aid requirements and ensure that they are produced in the proper format and aspect ratio for transmission;
d. Review and respond to user requirements for recordings;
e. Update training programs, as required, to reflect equipment modification, new equipment, or changes in operating procedures;
f. Develop procedures for and provide direct support to the USG Program Office senior leadership, ensuring complete AV and VTC support and quality of service for the duration of the service request;
g. To the extent possible, integrate AV and VTC customer support services with the USG Program Office customer services and service desk, providing a centralized service desk capability to track, coordinate, and deploy AV and VTC support;
h. Establish and maintain standard operating and usage procedures; and
i. Maintain current working knowledge of and implement the latest technological advances in AV, VTC, and other related topics

C.5.3.5 SUBTASK 3.5 – PROVIDE TELECOMMUNICATION O&M

The contractor shall provide the following telecommunication O&M support:

a. Maintain the classified and unclassified telecommunications capability in the facility and upgrade the telecommunications. The SITEC J contractor will support the network telecommunications infrastructure to include switches, routers, firewalls, etc. This typically does not include layer one infrastructure.;
b. Provide planning, engineering, implementation, and O&M support, as required by the Government, to SITEC J migration to new or advanced telecommunications solutions such as VOIP, Secure VOIP;
c. Provide site management and technical lead of O&M support to the command telecommunications infrastructure including switches, routers, firewalls. This typically does not include layer one infrastructure;
d. Maintain and operate command telecommunications equipment and tactical systems including switches, routers, and firewalls; and
e. Develop, update, and maintain technical and operational documentation as well as training materials (Section F, Deliverable 27) in order to facilitate knowledge transfer, troubleshooting, and requirements development

C.5.3.6 SUBTASK 3.6 – PROVIDE WEBSITE/PORTAL, DESIGN, DEVELOPMENT, OPERATIONS, AND MAINTENANCE

The contractor shall develop, implement, operate, and maintain all SITEC J portals as requested by the Government. The contractor shall develop, operate, and maintain an open collaborative portal to access centralized data, collaborate, share information and improve access to products and services for DoD. The contractor shall create MS SharePoint sites utilizing advanced SharePoint features. The contractor shall implement security requirements for DoD and IC portals and provide access to external users as requested. The contractor shall implement applications and content databases according to DISA, DoD, and IC requirements for SharePoint implementation. The contractor shall integrate solutions and support data release to and collaboration with approved users of SITEC J portals.

As required by the USG Program Office TPOC, the contractor shall provide portal design, integration, implementation and O&M by performing the following:

a. Design, integrate, implement, and administer SharePoint portals and related systems;
b. Provide continuous improvement processes to each portal to maintain their utility to DoD, IC, SITEC J and other users; and
c. Support refresh, redesign, consolidation, migrations, and other efforts to improve operations

As required by the USG Program Office TPOC, the contractor shall provide content management support by performing the following**:**

a. Implement, operate and maintain portal and website instances for the USG Program Office internally and externally accessible sites for unclassified networks, Secret networks, and TS networks;
b. Derive and analyze customer requirements, translating them into web design steps, web page formats, and file and directory structures;
c. Participate with other staff members in fine tuning data structures and to support information and decision systems;
d. Implement portal solutions (SharePoint and related applications) on approved IT platforms and baselines provided by SITEC J IT operations;
e. Collaborate with content owners to perform content management and support the continual refresh and maintenance of SITEC J portal content;
f. Integrate identity management and access control solutions as required to authenticate and manage user access to SITEC J portals;
g. Provide portal-related support and administration for other systems of record both internally to the USG Program Office and externally to DoD (These may include mission-specific portals and other business applications.);
h. Provide application-level administration of web and SharePoint servers and any related applications and features, including web pages and databases. Contractor personnel shall execute and follow SITEC J privileged user agreements and follow privilege management efforts enforced by the USG Program Office IT and CS personnel;
i. Support the Government’s development, implementation, and management of data migration strategies to move approved data from file servers and other storage locations to portals;
j. Support the development, implementation, and maintenance of a metadata storage solution for SITEC J Enterprise Information;
k. Perform portal software updates and upgrades IAW the CS requirements;

l. Plan and execute migration to DoD and IC enterprise services for SITEC J portals, content, and related systems in coordination with SITEC J enterprise IT objectives;
m. Provide full Integration with MS Office products (i.e., Word, PowerPoint, Excel, Outlook, Project, and Visio) that are heavily used by the USG Program Office staff;
n. Support the development of CS risk management packages and other documentation to satisfy the USG Program Office, DoD, and IC requirements;
o. Ensure compliance with website and portal-related CS and technical standards, guidelines, and frameworks for the DoD and IC in collaboration with SITEC J security engineers, testers, and risk management officials;
p. Support planning and implementation of security testing, remediation measures, and POA&M actions, including support to readiness reviews, audits, and other testing activities;
q. Perform studies and recommend technical architecture, design, and structure of portal infrastructure;
r. Collect, analyze, and report portal service usage and performance statistics;
s. Participate in and support technical meetings with Government and industry personnel;
t. Coordinate portals and related technology with the USG Program Office COOP/DR solutions, ensuring that SITEC J portals are accommodated in and compatible with COOP/DR solutions;
u. Perform unit testing, integration testing, functional testing, and quality control as needed to ensure proper operation of portal systems and functionality;
v. Perform trouble shooting, debugging, performance analysis, and error correction and resolve functional issues with websites and portals; and
w. Coordinate scheduled and unscheduled outages with SITEC J configuration management personnel and service desk personnel and the USG Program Office TPOC (This includes advanced notice of scheduled outage notifications and reporting of unscheduled outages.)

As required by the USG Program office TPOC, the contractor shall provide releasable portal support by performing the following:

a. Collection of requirements and implementation of solutions to enable collaboration and data sharing within SITEC J portals and websites that meets DISA, DoD, and IC requirements;
b. Implementation of identity management, access controls, and data management solutions to ensure that data access is granted only to authorized personnel; and
c. Coordination with CS personnel, and other personnel to define release and access policies, document policy, and technical implementation, and enable auditing and other security measures as required

C.5.3.6.1 SUBTASK 3.6.1 – PROVIDE WEB/PORTAL APPLICATION DEVELOPMENT AND ENGINEERING

As required by the USG Program Office TPOC, the contractor shall provide the following support to the Government's web/portal application design and development efforts:

a. The contractor shall collect requirements from internal and external customers and for development of SITEC J business applications and other portal-related applications. The contractor shall plan, design, develop, test, implement, and maintain portal-related applications and systems. The contractor shall support web development using MS Visual Studio, ASP, .NET, Structured Query Language (SQL) and Java and other tools/software as required.

The contractor shall perform the following services as requested by the Government and in direct collaboration with Government technical managers and branch chiefs:

a. Serve as web applications developer and programmer for SITEC J;
b. Lead the research, development, testing, and integration in the design of web-based applications in the management of enterprise data;
c. Develop web parts to enhance SharePoint site and site collection functionality and user experience; develop workflows; develop link and merge and aggregate custom views for various data sources; and establish metadata fields with document sets, internal and external content types;
d. Support development and integration of dashboards and management reporting tools for SITEC J IT functions such as CS, independent testing, network management, project trackers, and other functions that may require portal-based collaboration and reporting capabilities;
e. Perform studies, requirements gathering, and analysis and recommend technical design and structure of portal applications, systems, and services; serve as web applications developer and programmer for SITEC J;
f. Test, evaluate, and implement new web-based applications;
g. Resolve and troubleshoot specific and complex issues involved in the design and ongoing support of SITEC J websites and portals;
h. Develop new methods and criteria to document and implement web applications;
i. Design, develop, troubleshoot, debug, and implement web applications using current technologies;
j. Study customer requirements, translating them into web design steps, web page formats, and file and directory structures; and
k. Participate with other staff members in fine-tuning data structures to support information and decision systems

C.5.3.6.2 SUBTASK 3.6.2 – PROVIDE TECHNICAL DOCUMENTATION SUPPORT

The contractor shall create portal engineering and architecture documentation, user documentation, configuration and restoration plans, development/test/integration process documents and a portal administration guide. Each required document will be submitted to the USG Program Office TPOC for acceptance and approval for release.

For example, as required by the USG Program Office TPOC, the contractor shall perform the following:

a. Maintain documentation for system design, architecture, network connectivity, configuration settings, software versions, and custom SITEC J/user developed applications (Section F, Deliverable 27) for each instance of the SITEC J portal or website;

b. Prepare briefing materials, technical reports, roadmaps, implementation plans, risk management package components, and other technical documentation (Section F, Deliverable 17);

c. Deliver technical portal user guides, administrative guides, and training materials (Section F, Deliverable 25);

d. Document and report test plans, procedures, and results (Section F, Deliverable 30);

e. Support the Government development of a portal restoration/recovery plan in coordination with the USG Program Office engineers and the USG Program Office COOP/DR solutions; and

f. Support the Government development document portal-related policies and procedures

C.5.3.6.3 SUBTASK 3.6.3 – PROVIDE LEGAL DISCOVERY SEARCHES

The contractor shall provide the following legal discovery search support:

a. Execute searches for records throughout the command's collaborative environments to include SharePoint, files shares, Outlook and various other platforms;
b. Provide timely and accurate search results in response to legal discovery requests from Joint Staff and SOCOM;
c. Report findings to directorate leadership on issues, and status of on-going requests; and
d. Manage historical information on the execution of assigned requests for quality assurance

C.5.4 TASK 4 – PROVIDE DEPLOYED IT CAPABILITIES

The contractor shall provide robust, flexible, secure, and sustained end-to-end deployed IT capabilities. The contractor shall provide 24x7x365 phone response and remote support to deployed users of SITEC J expeditionary capabilities. The contractor shall tailor capabilities to meet the unique mission requirements and shall provide logistical support to ensure that capabilities are delivered by the mission-requirement date. The contractor shall support continuous improvement and identify efficiencies for improved capabilities for deployed users. The contractor shall maintain proficiency with deployed IT capabilities and knowledge of each system's configuration sufficient to provide step-by-step remote assistance for all aspects of system assembly, connection, operation, problem resolution, and disassembly.

C.5.4.1 SUBTASK 4.1 – PROVIDE DEPLOYED IT CAPABILITY INTEGRATION

The contractor shall provide support including assembly, integration, O&M, pre-deployment training, logistics, shipping, and Tier II and III technical support as well as Tier II and III *remote* user support. The contractor shall track and report status and location of all deployed IT capabilities and associated equipment. The contractor shall provide complete deployed IT capabilities lifecycle management, shall maintain bench stock and spare parts for repairs and kit refurbishment, and shall manage lifecycle replacements for aging or damaged kits.

Deployed IT capability lifecycle support includes the following:

a. Assessing IT infrastructure, mission, operational, communications requirements and unique Tactics, Techniques, and Procedures (TTP) for each deployed IT capability deployment location;

b. Assessing operational readiness and mission worthiness of each deployed IT capability. Identify and implement, with Government approval, options to mitigate the risk of equipment failure upon deployment;
c. Identifying necessary equipment, telecommunications, encryption, and bandwidth requirements and provide cost estimates where required;
d. Following the USG Program Office CM procedures, support Configuration Review Board (CRB) process;
e. Integrating all equipment and telecommunications capabilities required to support the mission at the target location;
f. Closely coordinating and cooperating with the Government in the handling of GFE through directed sources such as DISA;
g. Supporting RMF activities in collaboration with the USG Program Office CS and IT personnel to ensure deployed IT capability compliance, approved software images, and authorizations to operate and connect to SITEC J enterprise; and
h. Providing ad hoc design and other documentation (Section F, Deliverable 42) necessary to obtain authorization to operate and connect deployed IT capabilities to Government networks

C.5.4.2 SUBTASK 4.2 – PROVIDE TECHNICAL AND LOGISTICS SUPPORT FOR DEPLOYED IT CAPABILITIES

The contractor shall perform the following logistics, shipping, and reporting activities:

a. Conduct pre-deployment receipt and inspection of all IT equipment, documentation, shipping containers, and other material that will be deployed in support of the SITEC J analytical teams;
b. Provide secure and survivable packaging, handling, shipping, transportation and logistics to deliver deployed IT capabilities to approved destinations using DoD or commercial shipping methods, as required by the Government;
c. Provide remote, reach-back technical support for in-theater receipt, inspection, set-up, and disassembly to ensure the deployed IT capability is functional and meets approved acceptance criteria. In-theater support may be required upon Government approval of Temporary Duty (TDY);
d. Provide Tier II and Tier III Government-site user technical support. The contractor shall provide on-call phone support after hours to deployed users in *remote* locations, including users operating in potentially austere or hazardous conditions with no local IT or communications support. The contractors shall maintain proficiency with deployed IT capabilities and knowledge of each system's configuration sufficient to provide step-by-step remote assistance with all aspects of system assembly, connection, operation, and disassembly;

C.5.4.3 SUBTASK 4.3 – PROVIDE TRAINING

The contractor shall provide hands-on, system-specific training to familiarize users with the assembly, operation, disassembly, and inventory control of deployed IT capabilities at Site S, JCU and N2 as well as other sites that may be designated by the Government. The objective of training is to maximize the effectiveness of SITEC J support to the warfighter and to reduce end-user dependence on reach-back support while in remote operating areas. The contractor shall provide training materials, electronic and hard-copy user guides, reach-back support instructions, and other materials to meet mission requirements (Section F, Deliverable 33).

C.5.4.4 SUBTASK 4.4 – PROVIDE TELECOMMUNICATIONS, SATELLITE LINE OF SIGHT ENGINEERING SUPPORT

In support of SITEC J deployed IT capabilities, the contractor shall support, and maintain wireless, satellite, and communications capabilities in response to mission requirements. The Government connects to multiple terminals with the responsibility to create configuration files for deployments. For example, the contractor shall integrate and maintain mobile/portable satellite communications systems to ensure that deployed IT capabilities are self-contained to support deployed forces operating in remote locations. The contractor shall provide telecommunications user support and reach-back capabilities.

The contractor shall provide a Deployed IT Telecommunications and Satellite Requirements Report (Section F, Deliverable 34) that includes cost and functional analysis, assessments, risks, and courses of action to meet deployed or mobile user telecommunication requirements.

C.5.5 TASK 5 – PROVIDE GLOBAL COMMAND AND CONTROL SYSTEM (GCCS) AND AIR DEFENSE SYSTEM INTEGRATOR (ADSI) SUPPORT (OPTIONAL TASK)

The contractor shall provide IT technical services in support of the areas for mission programs interfacing with the following systems:

a. Global Command and Control System – Joint (GCCS-J) COP; and
b. Air Defense System Integrator (ADSI) COP

Additionally, the contractor shall support telecommunications and Communications Security (COMSEC), desktop and network engineering, system administration and user support, architecture, and CS in support of GCCS-J and ADSI.

IT project support services shall include the following:

a. Connection, integration, and SITEC J IT capabilities with the enterprise;
b. Migration of internally-hosted services to a Government enterprise service;
c. Providing proofs of concept, prototyping, and implementation of new or advanced IT capabilities, commercial products, and CS solutions; and
d. Providing rapid implementation and risk-management support of new IT capabilities
e. Collaboration with the USG Program Office J2 and watch operations to enable a fully integrated and coordinated user support experience that is easily accessible 24x7x365 for users of deployed IT capabilities;
f. Coordination with the USG Program Office J2 to manage map and imagery file archives and databases and assist J3 in maintaining uninterrupted access to the most current map and imagery files as well as assist Command Operational Picture (COP) operators import, display, and build map and imagery-based displays for current operations;

g. Coordination the employment of Blue Force Tracker (BFT) devices with the Army Space Command (ARSPACE) Space-Based Blue Force Tracking (SB-BFT) Mission Management Center (MMC) and shall ensure that the BFT database is updated with correct track names; and
h. Support to the Government development of capability status reports (e.g., operational readiness, deployment location, functional capabilities, training schedules) and other information to support the USG Program Office leadership

C.5.6 TASK 6 – PROVIDE SURGE SUPPORT (OPTIONAL TASK)

The contractor shall provide the ability to rapidly scale services and capabilities within the scope of this TO in response to emerging requirements locally, globally, and with SITEC J mission partners. Unpredictable world events demand that the USG Program Office maintain the capability to provide additional as needed support in CONUS and OCONUS, including deployment and Hazardous Duty/Combat Zones (HD/CZ) anywhere in the world. As required by the FEDSIM COR and the USG Program Office TPOC, and approved by the FEDSIM CO, the contractor shall provide additional as needed support within the scope of this TO anywhere in the world and on very short notice (often 30 days or less). Requirements for support may be generated by organizational changes, new SITEC J initiatives, decisive efforts, evolving mission requirements, emerging problem sets, and inter-agency collaboration and support agreements.

Services performed under this surge task may include any services within the scope of this TO and may be variable in length and level of effort. Additional as needed support may be project-based or result in long-term increase in base level of effort. Surge support may also require either short-term (up to two months) or longer-term deployments.

Surge support shall not result in a decrease of support to other TO requirements unless approved by the FEDSIM CO and COR.

The following applies to the performance of SITEC J surge support:

a. The Government will determine the amount of surge support required at the time of the situational action matter. Each situational action matter may require a different amount and length of support in order to meet specific requirements. When the first surge requirement is identified by the Government, the optional surge CLIN will be exercised. The CO will provide the contractor with a requirements document specifying the surge requirement, and expected outcomes.

b. The contractor shall develop a Surge Plan (Section F, Deliverable 43) upon request by the FEDSIM CO which shall include, project approach, milestones and schedules, and detailed resource information to be reviewed and approved by the Government.
c. The contractor shall provide surge support in identified situational action matters with the urgency the matter entails.

Once a situational action matter has been declared ended or the additional response support is no longer needed, the contractor shall proceed with an orderly and efficient scale down period NTE 30 days. During the scale down period, the contractor shall fully cooperate and assist the Government with activities closing out the action matter, developing required documentation, transferring knowledge, and documenting lessons learned.